

Verifying Computations using Zero-Knowledge Proofs

Advisor: **Anisha Mukherjee & Selim Kirbiyik**

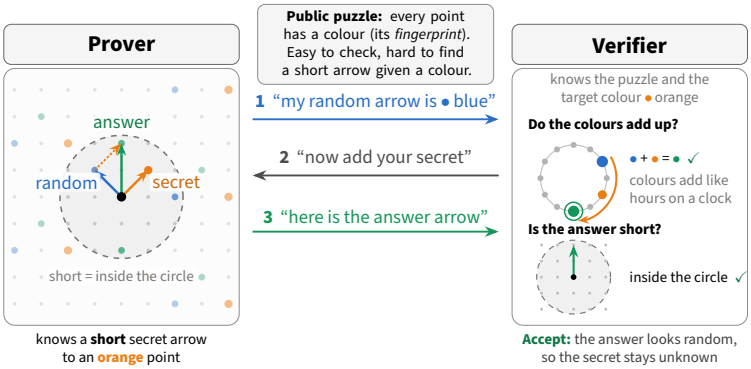
Motivation

Zero-Knowledge Proofs (ZKPs) are an advanced cryptographic primitive that allows a party to prove with high confidence that they hold a secret witness. ZKPs are currently used for proving you know your password without sharing it or solving less CAPTCHAs by keeping your anonymous proof that you are a human.

In this project you will answer the question 'How well does a lattice-based proof system perform?'. A proof system can be measured on multiple axis. Its proof size, prover time, verifier time, whether it is zero-knowledge, the hard problem it assumes, and what types of relations it supports natively.

Goals and Tasks

- Survey one lattice-based proof system
- Profile the existing implementation
- Identify which applications it is more suitable



Abstract view of a Lattice-based ZKP.

Literature

- H. Perez
  Lattice-Based ZK Explained
  2025
  zkv.xyz/lattice-based-zk-explained/

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM ☑ MATH

Prerequisites

- Interest in lattice-based cryptography
- Programming (C/C++, Python)

Advisor Contact

firstname.lastname@tugraz.at